Internal Audit's Control Bulletin for Management

GOT PASSWORD CONTROLS?

Did You Know?

Passwords such as someone's name, birth date, or a word from the dictionary may be easier to remember, but they're also very easy to break. It only takes one such password on a network to make it vulnerable to intruders.

Tips for Protecting Your Password

- Passwords should be changed periodically, about every 30 to 90 days. The more sensitive the data or the function, the more frequently passwords should be changed.
- A minimum length of 6-8 characters should be used for passwords so that they cannot be easily guessed.
- Use of alphanumeric passwords is encouraged since they are more difficult to guess.
- Do not give your password to anyone.
- Use a screensaver when you leave your computer. Remember, you are responsible for any activity associated with your User ID and password.

Internal Audit's role includes proactive activities such as providing helpful educational material (cash handling classes, audit classes, presentations) and now this new publication for management.

CIO Comments on Information Security

Lin Thatcher

In every government area, information technology is essential to conducting business with citizens, business partners and between agencies. Managers and employees at all levels require timely access to reliable information for routine operations and major decisions. The usefulness of this information depends upon availability, integrity, and protection of our information technology systems.

A reminder that County policy A1605 'Electronic Information Resources Security' informs us that "information" is a County asset and must be appropriately evaluated and protected against unauthorized use, disclosure, theft, modification, destruction, or denial of access. It further states that the protection and security of information resources is the responsibility of each Department Head and all employees.

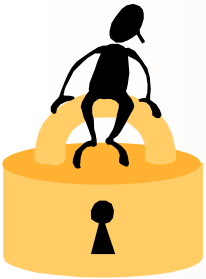
It is essential that each Department Head establish security controls and practices sufficient to ensure that the confidentiality (to the extent required by law), integrity, availability, recoverability, and appropriate use of all electronic data and information assets is maintained. They should create and adopt a departmental security policy for information, information systems, and for the transmission of information.

Beyond our own departments, all contracts and agreements with service providers or outside agencies that process information using a computer system on behalf of Maricopa County shall require compliance with the Electronic Information Resource Security Principles document.

FUTURE:
Biometrics—your thumb print may replace your password in the future

Although this end of the business seems rather dry and boring, it is nevertheless critical that we remain vigilant in taking the necessary steps to protect our business operations from unwanted, disruptive, and potentially embarrassing intrusions.

$$$ Security Breaches Can Be Costly $$$



In a joint survey by the FBI and the Computer Security Institute of San Francisco, 64% of 520 Fortune 500 companies, government organizations, and financial institutions reported security breaches over a 12-month period. The 241 organizations that attempted to quantify the financial impact of those computer crimes reported more than $136 million in losses.

Contact Internal Audit for internal control advice at (602) 506-1585